JOURNAL OF NUMBER THEORY 5, 271–286 (1973)

Residuacity Properties of Real Quadratic Units

JACOB A. BRANDLER*

Department of Mathematics, Bucknell University, Lewisburg, Pennsylvania 17837

Communicated by H. B. Mann

Received May 10, 1971

Necessary and sufficient conditions for representing certain classes of primes by given quadratic forms are found by generalizing techniques of rational number theory. The main result is that if $m = 5$ or 13, and if p is a rational prime such that $(-1/p) = 1 = (m/p)$, then a necessary and sufficient condition that $x^2 + 4my^2 = p$ for some rational integers x and y is that $[\epsilon_m/\mathfrak{p}] = 1$, where ϵ_m denotes the fundamental unit of the field $Q(m^{1/2})$ and $[\ /\ ]$ denotes the Legendre symbol of the ring of integers of $Q(m^{1/2})$ with $\mathfrak{p}$ a prime ideal divisor of p in $Q(m^{1/2})$.

1. INTRODUCTION

In their joint paper [1], Barrucand and Cohn proved the following result.

THEOREM. *Let ζ be a primitive eighth root of unity, and let $Q(\zeta)$ be the biquadratic extension of the rational field Q generated by ζ. Then the special primes p of the form $x^2 + 32y^2$ are distinguished from other (positive) primes $\equiv 1 \pmod 8$ by the property that all totally real units in $Q(\zeta)$, particularly $1 + \sqrt{2}$, are quadratic residues of π, any prime factor of p in $Q(\zeta)$.*

Stated differently, this theorem says that if p is an odd prime such that $(-1/p) = 1 = (2/p)$, then the solvability or unsolvability in $Q(\sqrt{2})$ of the congruence

$$\alpha^2 \equiv 1 + \sqrt{2} \pmod{\pi},$$

where π is a prime divisor of p in $Q(\sqrt{2})$ and α is an algebraic integer in $Q(\sqrt{2})$, determines how p shall be represented as the norm of some

* This paper is based on the author's dissertation, which was done at the University of Arizona.

algebraic integer in $Q(\sqrt{-2})$. Thus information obtained in one quadratic field gives us information of what is going on in a second quadratic field.

The question arises as to whether the above theorem can be extended to other pairs of quadratic fields. Namely, if m is a square-free natural number and ϵ_m denotes the fundamental unit of the real quadratic field $Q(m^{1/2})$, does the solvability or unsolvability of the congruence

$$\alpha^2 \equiv \epsilon_m \pmod{\mathfrak{p}},$$

where $\mathfrak{p}$ is a prime ideal divisor in $Q(m^{1/2})$ of the odd rational prime p satisfying $(-1/p) = 1 = (m/p)$, tell us how p can be represented by norms in $Q((-m)^{1/2})$.

We obtain some results along these lines if we restrict m to be a prime $\equiv 1 \pmod 4$ by methods which are in most instances generalizations of techniques used in rational number theory.

2. The Principal Residuacity Relation

Let m be a positive rational prime, $m \equiv 1 \pmod 4$. Let

$$K = Q(m^{1/2}, (-m)^{1/2}) = Q(m^{1/2} + (-m)^{1/2})$$

denote the so-called special Dirichlet biquadratic field generated by $m^{1/2}$ and $(-m)^{1/2}$ (see [3]). Let $k = Q(i)$, $k_1 = Q(m^{1/2})$, and $k_2 = Q((-m)^{1/2})$ denote the three quadratic subfields of K. Let $\mathscr{Z}[i]$ denote the ring of integers of k, and let O_j denote the ring of integers of k_j, $j = 1, 2$ (see [2]). Elements in the unique factorization domain $\mathscr{Z}[i]$ will be denoted by lower case Greek letters. Prime ideals in O_1 will be denoted by lower case script letters, and prime ideals in O_K will be denoted by upper case script letters. We assume as known the facts on quadratic residuacity in algebraic extensions of Q (see [4]).

Now let p be a rational prime such that $(-1/p) = 1 = (m/p)$, where $(\ /\ )$ denotes the Legendre symbol for rational integers. In $\mathscr{Z}[i]$, the primes p and m can be factored as the product of two Gaussian primes, $p = \pi\bar{\pi}$ and $m = \mu\bar{\mu}$, where $^-$ denotes complex conjugate; furthermore, p can be factored as the product of two prime ideals in O_1, $p = \mathfrak{p}\mathfrak{p}'$, where $'$ denotes the conjugacy operation in O_1.

The main result of this section is that

$$[\epsilon_m/\mathfrak{p}] = [\mu/\pi],$$

where $[\ /\ ]$ on the left and right sides, respectively, denotes the Legendre symbol in O_1 and $\mathscr{Z}[i]$, and ϵ_m is the fundamental unit of k_1.

To prove this result, which is Theorem 1, Corollary 2 below, we need a lemma. But before we proceed, we must make a few observations. First, if $\epsilon_m = x + ym^{1/2}$ is the fundamental unit in k_1, then ϵ_m and ϵ_m^3 have the same residuacity character with respect to a prime ideal. Second, if x and y are not integers, then ϵ_m^3 does have integral coefficients. In order to avoid fractions, we will temporarily let $\epsilon_m = x + ym^{1/2}$, where the integer pair x, y denotes the fundamental solution of the Diophantine equation

$$X^2 - mY^2 = -1,$$

and we shall refer to ϵ_m as the *fundamental integral unit* of k_1. Now we proceed to our lemma.

LEMMA 1. *If $\epsilon_m = x + ym^{1/2}$ is the fundamental integral unit of $k_1 = Q(m^{1/2})$, $m \equiv 1 \pmod 4$ a rational prime, then there exists a pair, α, β, of Gaussian integers such that*

$$y = \alpha\beta \qquad \text{and} \qquad 2x = \mu\alpha^2 + \bar{\mu}\beta^2,$$

where $\mu, \bar{\mu}$ are in $\mathscr{Z}[i]$ satisfying $\mu\bar{\mu} = m$.

Proof. First we will find α, β in $\mathscr{Z}[i]$ satisfying

$$\mu\alpha^2 - \bar{\mu}\beta^2 = -2i.$$

$\epsilon_m = x + ym^{1/2}$ is the fundamental integral unit in k_1, where x and y are integers satisfying

$$x^2 - my^2 = -1.$$

Hence,

$$my^2 = (x + i)(x - i),$$

since $\mathscr{Z}[i]$ is a unique factorization domain. Clearly, x is an even integer and y is an odd integer. Furthermore, $x + i$ and $x - i$ are relatively prime Gaussian integers, for if they had a common divisor other than one or a unit of $\mathscr{Z}[i]$, then necessarily they would have $1 + i$ as a factor implying $(x + i)(x - i)$ is divisible by 2; since both m and y are odd integers, we have a contradiction. Therefore, $(x + i, x - i) = 1$, and one of the following two sets of equations must hold

$$x \pm i = \alpha^2, \qquad x \mp i = m\beta^2, \qquad y = \alpha\beta, \qquad \alpha, \beta \text{ in } \mathscr{Z}[i]; \tag{1}$$

$$x - i = \mu\alpha^2, \qquad x + i = \bar{\mu}\beta^2, \qquad y = \alpha\beta, \qquad \alpha, \beta \text{ in } \mathscr{Z}[i], \quad \mu\bar{\mu} = m. \tag{1'}$$

By considering conjugates, (1) is evidently impossible, which leaves (1′) as the only remaining possibility. Therefore, (1′) implies

$$\mu\alpha^2 - \bar{\mu}\beta^2 = 2i.$$

Now, to prove our lemma, we know that since $\epsilon_m = x + ym^{1/2}$ is the fundamental integral unit of k_1, then

$$x^2 - my^2 = -1$$

or

$$4x^2 = -4 + 4my^2.$$

From above we know that Gaussian integers, α, β, exist such that

$$y = \alpha\beta \qquad \text{and} \qquad \mu\alpha^2 - \bar{\mu}\beta^2 = -2i.$$

Hence,

$$\begin{aligned}(\mu\alpha^2 + \bar{\mu}\beta^2)^2 &= (\mu\alpha^2 - \bar{\mu}\beta^2)^2 + 4\mu\bar{\mu}\alpha^2\beta^2 \\ &= -4 + 4my^2 \\ &= 4x^2.\end{aligned}$$

Therefore,

$$\mu\alpha^2 + \bar{\mu}\beta^2 = 2x.$$

THEOREM 1. *Let $\epsilon_m = x + ym^{1/2}$ be the fundamental integral unit of $k_1 = Q(m^{1/2})$, where $m \equiv 1 \pmod 4$ is a positive rational prime. Let $K = Q(m^{1/2}, (-m)^{1/2})$. Let μ, $\bar{\mu}$ be elements of $\mathfrak{Z}[i]$ such that $\mu\bar{\mu} = m$. Then ϵ_m is a perfect square in O_K.*

Proof. By Lemma 1 there exist Gaussian integers α, β such that

$$y = \alpha\beta \qquad \text{and} \qquad 2x = \mu\alpha^2 + \bar{\mu}\beta^2.$$

Therefore,

$$\begin{aligned}2\mu\epsilon_m &= 2\mu(x + ym^{1/2}) = 2\mu x + 2\mu ym^{1/2} \\ &= \mu(\mu\alpha^2 + \bar{\mu}\beta^2) + 2\mu\alpha\beta m^{1/2} \\ &= (\mu\alpha + \beta m^{1/2})^2.\end{aligned}$$

Hence,

$$\begin{aligned}-i(1+i)^2\,\mu\epsilon_m &= (\mu\alpha + \beta m^{1/2})^2 \\ -i\mu\epsilon_m &= \{(\mu\alpha + \beta m^{1/2})/(1+i)\}^2,\end{aligned}$$

where the right side is clearly an integer since $\alpha \equiv \beta \equiv \mu \equiv 1 \pmod{1+i}$, and obviously $m \not\equiv 0 \pmod{1+i}$ in O_K. $-i\mu = \hat{\mu}$ is an associate of μ. Since this particular factorization (with respect to associates) of m in $\mathscr{Z}[i]$ is irrelevant, we may replace $\hat{\mu}$ by μ, so that we finally obtain

$$\mu\epsilon_m = \{(\hat{\mu}\alpha + \beta m^{1/2})/(1+i)\}^2.$$

COROLLARY 1. *If ϵ_m denotes the fundamental unit of $k_1 = Q(m^{1/2})$ (rather than the fundamental integral unit) and the remaining hypotheses of Theorem* 1 *are left unaltered, then $\mu\epsilon_m$ is a square in O_K.*

Proof. This clearly follows from Theorem 1 and our remarks preceding Lemma 1.

COROLLARY 2. *If p is an odd positive rational prime such that $(-1/p) = 1 = (m/p)$, if $\mathfrak{p}$ is a prime ideal divisor of p in O_1, and if π is a prime factor of p in $\mathscr{Z}[i]$, then*

$$[\epsilon_m/\mathfrak{p}] = [\mu/\pi],$$

where [/] on the left side denotes the Legendre symbol in O_1 and [/] on the right side denotes the Legendre symbol in $\mathscr{Z}[i]$.

Proof. For the purpose of this proof, let $\langle\ /\ \rangle$ denote the Legendre symbol of the field $K = Q(m^{1/2}, (-m)^{1/2})$. Since $(-1/p) = 1 = (m/p)$, it follows that the prime ideal $\mathfrak{p}$ of O_1 splits as the product of two relatively prime ideals $\mathfrak{P}$, $\mathfrak{P}'$ in O_K, and the prime π of $\mathscr{Z}[i]$ factors as the product of two relatively prime ideals $\mathfrak{P}$, $\mathfrak{P}''$ in O_K, that is

$$\mathfrak{p} = \mathfrak{P}\mathfrak{P}' \qquad \text{and} \qquad (\pi) = \mathfrak{P}\mathfrak{P}'',$$

(see Hilbert [4]). Hence,

$$[\epsilon_m/\mathfrak{p}] = \langle \epsilon_m/\mathfrak{p} \rangle = \langle \epsilon_m/\mathfrak{P} \rangle = \langle \mu/\mathfrak{P} \rangle = \langle \mu/\pi \rangle = [\mu/\pi],$$

where the third equality is a consequence of Theorem 1.

3. A Result of Mrs. Emma Lehmer

Before proceeding with the main application of Theorem 1 and Corollary 2, we present an elementary proof of a theorem due to Mrs. Emma Lehmer.

THEOREM 2. *Let p and q be positive primes such that $p \equiv q \equiv 1 \pmod 4$, $(p/q) = 1$. Let $\mathfrak{p}$ be a prime ideal divisor of p in $Q(q^{1/2})$, and let $\mathfrak{q}$ be a prime ideal divisor of q in $Q(p^{1/2})$. Then*

$$[\epsilon_p/\mathfrak{q}] = [\epsilon_q/\mathfrak{p}],$$

where ϵ_p, ϵ_q denote the fundamental units of $Q(p^{1/2})$, $Q(q^{1/2})$, respectively, and $[\ /\ ]$ on the left and right sides denote the residuacity symbols in $Q(p^{1/2})$ and $Q(q^{1/2})$, respectively.

Proof. Let π and λ denote prime divisors of p and q in $\mathscr{Z}[i]$, respectively, with $\mathrm{Im}(\pi)$ and $\mathrm{Im}(\lambda)$ even. Then by Theorem 1, Corollary 2, and the law of quadratic reciprocity in $\mathscr{Z}[i]$, we have

$$[\epsilon_p/\mathfrak{q}] = [\pi/\lambda] = [\lambda/\pi] = [\epsilon_q/\mathfrak{p}],$$

where $[\ /\ ]$ on the inside of these equations denotes the Legendre symbol in $\mathscr{Z}[i]$.

4. SOME PREPARATORY LEMMAS

In order to proceed with our applications, we must make some observations about the ring of Gaussian integers, $\mathscr{Z}[i]$, and state one lemma about quadratic forms over $\mathscr{Z}$. Let α be in $\mathscr{Z}[i]$; α is said to be *even* if $1 + i$ divides α; otherwise, α is said to be *odd*. If $\alpha = a + bi$ is in $\mathscr{Z}[i]$, then α is odd if and only if $a \not\equiv b \pmod 2$.

LEMMA 2. *Let $\alpha = a + bi$ in $\mathscr{Z}[i]$ be odd; then $\alpha^2 \equiv \pm 1 \pmod{\{1 + i\}^5}$.*

Proof. Trivial.

Lemma 2 remains valid if the exponent 5 is replaced by any natural number less than or equal to 5; we will frequently use this fact and refer to Lemma 2 as justification.

LEMMA 3. *Let d be in $\mathscr{Z}$, and let α and β be in $\mathscr{Z}[i]$. Then there exist rational integers x, y such that*

$$(\alpha^2 + d\beta^2)(\bar{\alpha}^2 + d\bar{\beta}^2) = x^2 + 4dy^2.$$

Proof. Let $x = \alpha\bar{\alpha} - d\beta\bar{\beta}$ and $y = Rl\{\alpha\bar{\beta}\}$ in the above equation and multiply the two sides of the above equation out.

LEMMA 4. *Let p be a rational prime and let d be any positive integer.*

If there exist natural numbers x and y such that $p = x^2 + dy^2$, then x and y are unique.

See Nagell [5] for a proof of a more general result of which Lemma 4 is a special case.

5. Applications

The following important lemma is the key to our applications. Although it can be stated more generally, we state it in the form in which we will use it.

Lemma 5. *Let d be a rational integer, and let π in $\mathscr{Z}[i]$ be a Gaussian prime such that $[-d/\pi] = 1$ and $N(\pi) = p$ is a rational prime. Then there exists a pair, ξ, η, of Gaussian integers such that $(\xi, n) = 1$ and*

$$\xi^2 + d\eta^2 = \gamma\pi,$$

where γ is a Gaussian integer. Furthermore,

$$|\gamma| < \begin{cases} |d| + 1, & \text{if } p > 34, \\ (3/4)(|d| + 1), & \text{if } p > 392. \end{cases}$$

Proof. Let ζ be a Gaussian integer satisfying

$$\zeta^2 \equiv -d \pmod{\pi}.$$

Consider the set of all Gaussian integers

$$\alpha - \zeta\beta,$$

where α and β run through all Gaussian integers such that

$$0 \leqslant |Rl\{\alpha\}|, \quad |\operatorname{Im}\{\alpha\}| \leqslant (p^{1/4} + 1)/2$$

and

$$0 \leqslant |Rl\{\beta\}|, \quad |\operatorname{Im}\{\beta\}| \leqslant (p^{1/4} + 1)/2.$$

There are

$$(1 + 2[(p^{1/4} + 1)/2])^4 > p = N(\pi)$$

different pairs α, β, where [ ] denotes the greatest integer function. Therefore, two distinct pairs, α_1, β_1 and α_2, β_2, must exist such that

$$\alpha_1 - \zeta\beta_1 \equiv \alpha_2 - \zeta\beta_2 \pmod{\pi}.$$

If we set $\alpha_2 - \alpha_1 = \xi$ and $\beta_2 - \beta_1 = \eta$, we have

$$\zeta\eta \equiv \xi \pmod{\pi},$$

with

$$|\xi|, |\eta| \leqslant (p^{1/4} + 1)/\sqrt{2}.$$

Clearly neither ξ nor η is equal to 0. We may, of course, assume $(\xi, \eta) = 1$. Then

$$\zeta^2\eta^2 \equiv \xi^2 \pmod{\pi}$$

$$\xi^2 + d\eta^2 = \gamma\pi,$$

for some γ in $\mathscr{Z}[i]$. Now

$$|\gamma\pi| = |\xi^2 + d\eta^2| \leqslant |\xi|^2 + |d||\eta|^2 \leqslant (1 + |d|)(p^{1/4} + 1)^2/(\sqrt{2})^2$$

Hence,

$$|\gamma| \leqslant (1 + |d|)(1 + p^{-1/4})^2/2.$$

If $p > 34$, then

$$(1 + p^{-1/4})^2 < 2,$$

and if $p > 392$, then

$$(1 + p^{-1/4})^2 < 3/2.$$

It is clear that this proves our lemma.

THEOREM 3. *Let p be a rational prime such that $(-1/p) = 1 = (m/p)$, $m = 5$ or 13. Let $\pi = a + bi$ in $\mathscr{Z}[i]$ be a Gaussian prime such that $N(\pi) = p$; assume throughout that b is even. Then there exist Gaussian integers ξ, η with $(\xi, \eta) = 1$ such that either*

$$\xi^2 + m\eta^2 = \epsilon\pi$$

or

$$\xi^2 + m\eta^2 = 2\epsilon\pi,$$

where $\epsilon = \pm 1$ or $\pm i$.

Proof. We will prove this theorem only for $m = 5$; for $m = 13$ the proof is analogous.

The smallest prime p such that $(-1/p) = 1 = (5/p)$ is $p = 29$. Since $29 = (5 + 2i)(5 - 2i)$ and

$$(3 + 2i)^2 + 5(1 - i)^2 = 5 + 2i,$$

we see that the theorem is true for all primes $p < 34$ satisfying $(-1/p) = 1 = (5/p)$. Consequently, we may assume $p > 34$. Then, by Lemma 5, there exists a pair, ξ, η, of Gaussian integers with $(\xi, \eta) = 1$ such that

$$\xi^2 + 5\eta^2 = \gamma\pi, \tag{2}$$

where $(N(\gamma))^{1/2} = |\gamma| < 6$, because

$$[-5/\pi] = (-5/p) = 1.$$

Then $N(\gamma) < 36$; therefore, the only possible values for $N(\gamma)$ are $N(\gamma) = 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34$. Now

$$N(\gamma)p = (\gamma\pi)(\bar{\gamma}\bar{\pi}) = (\xi^2 + 5\eta^2)(\bar{\xi}^2 + 5\bar{\eta}^2).$$

Thus, by Lemma 3, rational integers x, y exist such that

$$x^2 + 20y^2 = N(\gamma)p. \tag{3}$$

Since $(5/p) = 1 = (p/5)$, Eq. (3) implies $(N(\gamma)/5) = 1$. Hence,

$$N(\gamma) \neq 2, 8, 13, 17, 18, 32.$$

Next,

$$N(\gamma) \neq 10, 26, 34,$$

for otherwise 2 divides x in Eq. (3), which is impossible.

To consider the remaining possibilities for $N(\gamma)$, we return to the ring $\mathscr{Z}[i]$. We will show that if Eq. (2) is true when $N(\gamma) = 5, 9, 16, 20, 25, 29$, then there exists another pair ξ', η' of Gaussian integers such that either

$$\xi'^2 + 5\eta'^2 = \epsilon\pi \tag{4}$$

or

$$\xi'^2 + 5\eta'^2 = 2\epsilon\pi, \tag{4'}$$

where $N(\epsilon) = 1$.

First, let us consider the case $N(\gamma) = 9$. Then (2) becomes

$$\xi^2 + 5\eta^2 = 3\epsilon\pi, \tag{5}$$

where $N(\epsilon) = 1$. Note that

$$1^2 + 5 \cdot 1^2 = 6.$$

These latter two equations imply that

$$\{(\xi - 5\eta)/3\}^2 + 5\{(\xi + \eta)/3\}^2 = 6(3\epsilon\pi)/9 = 2\epsilon\pi.$$

We need only show that $(\xi + \eta)/3$ is in $\mathscr{Z}[i]$. But Eq. (5) implies

$$\xi^2 + 5\eta^2 \equiv 0 \pmod 3$$

$$\xi \equiv \pm\eta \pmod 3.$$

Without loss of generality, we may assume the sign of η is chosen such that

$$\xi \equiv -\eta \pmod 3,$$

which proves our claim.

Similarly, by using the identity

$$(1 + 2i)^2 + 5 \cdot 1^2 = 2(1 + 2i),$$

we can show that if $N(\gamma) = 20$, then Eq. (2) can be put into the form of Eq. (4'), and by using the identity

$$(3 + 2i)^2 + 5(1 - i)^2 = 5 + 2i,$$

we can show that if $N(\gamma) = 29$, then Eq. (2) can be put into the form of Eq. (4). If $N(\gamma) = 5$, we multiply both sides of Eq. (2) by $(1 + i)^2$ and proceed as in the case for $N(\gamma) = 20$. If $N(\gamma) = 25$, it is trivial to show that Eq. (2) can be transformed into an equation of type (4). This leaves only one case to consider.

Assume now that $N(\gamma) = 16$; then $\gamma = 4\epsilon$, $N(\epsilon) = 1$. Then Eq. (2) becomes

$$\xi^2 + 5\eta^2 = 4\epsilon\pi, \tag{6}$$

where $(\xi, \eta) = 1$. Therefore, both ξ and η are odd. Equation (6) implies

$$\xi^2 + \eta^2 \equiv 0 \pmod 4.$$

By Lemma 2

$$\xi^2 \equiv \pm 1 \pmod 4 \qquad \text{and} \qquad \eta^2 \equiv \pm 1 \pmod 4.$$

These three congruences imply

$$\xi^2 \equiv -\eta^2 \equiv \pm 1 \pmod 4. \tag{7}$$

We may choose ξ such that

$$\xi^2 \equiv 1 \pmod 4. \tag{8}$$

Congruences (7) and (8) together with Lemma 2 imply

$$\xi^2 + \eta^2 \equiv 0 \ (\mathrm{mod}\{1+i\}^5)$$
$$(\xi + i\eta)(\xi - i\eta) \equiv 0 \ (\mathrm{mod}\{1+i\}^5).$$

Therefore, by appropriately choosing the sign of η, we have

$$\xi + i\eta \equiv 0 \ (\mathrm{mod}\{1+i\}^3). \tag{9}$$

Hence,

$$\left(\frac{i\xi - 5\eta}{(1+i)^3}\right)^2 + 5\left(\frac{\xi + i\eta}{(1+i)^3}\right)^2 = \frac{(i^2+5)(\xi^2+5\eta^2)}{(1+i)^6}$$
$$= 4(4\epsilon\pi)/(-8i) = 2\epsilon'\pi,$$

where $N(\epsilon') = 1$; by (9), $(\xi + i\eta)/(1+i)^3$ is in $\mathscr{Z}[i]$.

This completes the proof of our theorem.

COROLLARY. *Let p be a rational prime such that $(-1/p) = 1 = (m/p)$, $m = 5$ or 13. Let π in $\mathscr{Z}[i]$ be a Gaussian prime such that $N(\pi) = p$ and $\mathrm{Im}(\pi)$ is even. Then there exist Gaussian integers, ξ, η, with $(\xi, \eta) = 1$ such that either*

$$\xi^2 + m\eta^2 = \epsilon\pi$$

or

$$\xi^2 + m\eta^2 = \mu\epsilon\pi,$$

where $\mu = 1 + 2i$ and $3 + 2i$, respectively, according as $m = 5$ and 13, and $N(\epsilon) = 1$.

Proof. As in the proof of Theorem 3, we will prove this statement only for $m = 5$.

From Theorem 3 it follows that it suffices to show that if

$$\xi^2 + 5\eta^2 = 2\epsilon\pi, \tag{10}$$

then we can find a pair, ξ', η' such that

$$\xi'^2 + 5\eta'^2 = (1+2i)\,\epsilon\pi.$$

Thus, assume Eq. (10) is valid; then ξ and η are both odd, since we may assume $(\xi, \eta) = 1$. Equation (10) implies

$$\xi^2 + 5\eta^2 \equiv 2\epsilon\pi \equiv 2\epsilon \ (\mathrm{mod}\ 4)$$
$$\xi^2 + \eta^2 \equiv 2\epsilon \ (\mathrm{mod}\ 4). \tag{11}$$

Since ξ and η are both odd, then, by Lemma 2,

$$\xi^2 \equiv \pm 1 \pmod 4 \qquad \text{and} \qquad \eta^2 \equiv \pm 1 \pmod 4,$$

which imply

$$\xi^2 + \eta^2 \equiv 0, 2 \pmod 4.$$

If

$$\xi^2 + \eta^2 \equiv 0 \pmod 4,$$

then this congruence together with (11) implies

$$2\epsilon \equiv 0 \pmod 4,$$

which is clearly false. Consequently,

$$\xi^2 + \eta^2 \equiv 2 \pmod 4,$$

which implies

$$\xi^2 \equiv \eta^2 \equiv \pm 1 \pmod 4.$$

This congruence, in turn, implies

$$\xi \equiv \pm \eta \pmod 2, \tag{12}$$

with both signs holding. Remembering that

$$(1 + 2i)^2 + 5 \cdot 1^2 = 2(1 + 2i), \tag{13}$$

then Eqs. (10) and (13) together imply

$$\{(1 + 2i)\xi + 5\eta\}^2 + 5\{\xi - (1 + 2i)\eta\}^2 = 4(1 + 2i)\,\epsilon\pi. \tag{14}$$

But congruence (12) implies

$$(1 + 2i)\xi + 5\eta \equiv \xi - (1 + 2i)\eta \equiv 0 \pmod 2.$$

Letting

$$(1 + 2i)\xi + 5\eta = 2\xi' \qquad \text{and} \qquad \xi - (1 + 2i)\eta = 2\eta',$$

then Eq. (14) becomes

$$\xi'^2 + 5\eta'^2 = (1 + 2i)\,\epsilon\pi.$$

THEOREM 4. *Let $\pi = a + bi$ in $\mathscr{Z}[i]$ be a Gaussian prime such that $N(\pi) = p$ is a rational prime; hence, $(-1/p) = 1$. Assume b is even. Finally assume $(m/p) = 1$, $m = 5$ or 13. Then*

$$[\mu/\pi] = \begin{cases} +1 \text{ if and only if } p = x^2 + 4my^2 \text{ for some } x, y \text{ in } \mathscr{Z}, \\ -1 \text{ if and only if } p = 4x^2 + my^2 \text{ for some } x, y \text{ in } \mathscr{Z}, \end{cases}$$

where $\mu = 1 + 2i$ or $3 + 2i$ according as $m = 5$ or 13.

Proof. Once again, we will prove our result only for the case $m = 5$. From Theorem 3 we know that there exist Gaussian integers, ξ, η, such that either

$$\xi^2 + 5\eta^2 = \epsilon\pi \tag{15}$$

or

$$\xi^2 + 5\eta^2 = 2\epsilon\pi, \tag{16}$$

where $N(\epsilon) = 1$. Assume $[1 + 2i/\pi] = 1$; then Eq. (16) is impossible. For if (16) is valid, then, since $[\pi/1 + 2i] = 1$ by the law of quadratic reciprocity in $\mathscr{Z}[i]$,

$$[2\epsilon/1 + 2i] = 1,$$

which is impossible if $\epsilon = \pm 1$. Assume, therefore, that $\epsilon = \pm i$. Equation (16) implies

$$\xi^2 + 5\eta^2 \equiv \pm 2i \pmod 4.$$

Since ξ, η are both odd, Lemma 2 implies

$$\xi^2 + 5\eta^2 \equiv 0, 2 \pmod 4,$$

and these latter congruences imply

$$+2i \equiv 0, 2 \pmod 4,$$

no one of which is valid. Thus, (16) is impossible. Therefore, if $[1 + 2i/\pi] = 1$, then Eq. (15) is true, which implies, by Lemma 3, that

$$p = x^2 + 20y^2.$$

Similarly, if $[1 + 2i/\pi] = -1$, then Eq. (15) is impossible, and, consequently, Eq. (16) is true. If Eq. (16) is true, then by the corollary of Theorem 3, there exist Gaussian integers, ξ', η', such that

$$\xi'^2 + 5\eta'^2 = (1 + 2i)\,\epsilon\pi. \tag{17}$$

By Lemma 3, there exist rational integers, z, x, such that Eq. (17) implies

$$z^2 + 20x^2 = 5p.$$

Therefore, 5 divides z, say $z = 5y$, and this last equation becomes

$$4x^2 + 5y^2 = p.$$

Conversely, let p be a prime of the form

$$x^2 + 20y^2 = p. \tag{18}$$

Then x is odd, and Eq. (18) implies

$$(-1/p) = 1 = (5/p).$$

If $p = a^2 + b^2$ and $\pi = a + bi$, b even, then

$$[-5/\pi] = 1,$$

so that Theorem 3 is applicable. If $[1 + 2i/\pi] = -1$, then, by the first part of this theorem, there exist rational integers, u, v, such that

$$4u^2 + 5v^2 = p. \tag{19}$$

Equations (18) and (19) together imply

$$x^2 + 5(2y)^2 = p = (2u)^2 + 5v^2,$$

which implies, by Lemma 4, that

$$| 2u | = | x |,$$

which is impossible, since x is odd. Therefore, we have a contradiction. Hence,

$$[1 + 2i/\pi] = +1.$$

Similarly, if $p = 4x^2 + 5y^2$, then $(-1/p) = 1 = (5/p)$, and

$$[1 + 2i/\pi] = -1,$$

where $\pi = a + bi$ and $p = a^2 + b^2$, b even.

THEOREM 5. *Let p be an odd, positive rational prime such that $(-1/p) = 1 = (m/p)$, $m = 5$ or 13. Let ϵ_m be the fundamental unit of*

$Q(m^{1/2})$. *Finally, let* π *be a prime divisor of* p *in* $\mathscr{Z}[\omega]$, *where* $\omega = (1 + m^{1/2})/2$. *Then*

$$[\epsilon_m/\pi] = 1 \qquad \text{if and only if} \quad p = x^2 + 4my^2,$$

where [/] *denotes the Legendre symbol of* $\mathscr{Z}[\omega]$.

Proof. This follows directly from Theorem 1, Corollary 2, and Theorem 4.

We now state two theorems, similar to Theorems 3, 4, and 5, for the number $m = 17$.

THEOREM 6. *Let* p *be a rational prime such that* $(-1/p) = 1 = (17/p)$; *let* $\pi = a + bi$ *in* $\mathscr{Z}[i]$ *be a Gaussian prime such that* $N(\pi) = p$, *and assume* b *is even. Then there exist Gaussian integers,* ξ, η, *such that either*

$$\xi^2 + 17\eta^2 = 4\epsilon\pi$$

or

$$\xi^2 + 17\eta^2 = 4(1 + i)\,\epsilon\pi,$$

where $\epsilon = \pm 1$ *or* $\pm i$.

THEOREM 7. *Let* $\pi = a + bi$ *in* $\mathscr{Z}[i]$ *be a Gaussian prime such that* $N(\pi) = p$ *is a rational prime; hence,* $(-1/p) = 1$. *Assume* b *is even. Then*

$$[1 + 4i/\pi] = \begin{cases} +1 \text{ if and only if } p = x^2 + 17y^2 \text{ for some } x, y \text{ in } \mathscr{Z}, \\ -1 \text{ if and only if } 2p = x^2 + 17y^2 \text{ for some } x, y \text{ in } \mathscr{Z}, \end{cases}$$

where [/] *denotes the residuacity symbol in* $\mathscr{Z}[i]$.

Also, if $\epsilon_{17} = 4 + \sqrt{17}$ *is the fundamental unit in* $Q(\sqrt{17})$, *and* π' *is a prime divisor of* p *in* $Q(\sqrt{17})$, *then*

$$[\epsilon_{17}/\pi'] = \begin{cases} +1 \text{ if and only if } p = x^2 + 17y^2 \text{ for some } x, y \text{ in } \mathscr{Z}, \\ -1 \text{ if and only if } 2p = x^2 + 17y^2 \text{ for some } x, y \text{ in } \mathscr{Z}, \end{cases}$$

where [/] *denotes the residuacity symbol in* $Q(\sqrt{17})$.

The proofs of these theorems, though tedious, are similar to the proofs of Theorems 3, 4, and 5. We close this section with the comment that the second part of Theorem 7 requires a result, similar to Lemma 4, which states that the two equations $x^2 + 17y^2 = p$ and $u^2 + 17v^2 = 2p$ cannot be solved simultaneously in rational integers for any prime p.

6. Concluding Remarks

As we stated in our introduction, our goal has been to find a relationship between the quadratic residuacity character of the fundamental unit ϵ_m of the real quadratic field $Q(m^{1/2})$, with respect to a prime ideal divisor of the rational prime p, $(-1/p) = 1 = (m/p)$, and the prime ideal divisors of p in $Q((-m)^{1/2})$. Theorems 5 and 7 may be expressed in such a form, but for larger values of m it is more convenient to state our results in terms of ideal theory rather than in terms of quadratic forms. Before we do this, however, we would like to point out that in all likelihood Theorem 5 can be extended to include the value $m = 37$, and Theorem 7 can be extended to include the values $m = 73$, 97, and 193; Mrs. Emma Lehmer has recently informed the author that she has proved these conjectures by different means. With the aid of the University of Arizona's IBM 1130, a limited study was made to determine in which quadratic fields the desired kind of relationship might exist. All positive primes $m < 300$ with $m \equiv 1 \pmod 4$ were examined. On the basis of our numerical survey, it was found that, excluding the values $m = 5$, 13, and 37, the only primes m for which a pattern occurred were those $m \equiv 1 \pmod 8$. On the basis of our numerical studies, we close this paper with the following conjecture.

Conjecture. *Let $m \equiv 1 \pmod 8$ be a positive rational prime, $m \neq 17$, 73, 97, and 193, and let ϵ_m denote the fundamental unit of the real quadratic field $Q(m^{1/2})$. Let p be an odd prime satisfying $(-1/p) = 1 = (m/p)$ and let $\mathfrak{p}$ and $\hat{\mathfrak{p}}$ denote prime ideal divisors of p in $Q(m^{1/2})$ and $Q((-m)^{1/2})$, respectively. Then $[\epsilon_m/\mathfrak{p}] = 1$ (in $Q(m^{1/2})$) if and only if $\hat{\mathfrak{p}}^4$ is a principal ideal in $Q((-m)^{1/2})$.*

We have excluded the four values $m = 17$, 73, 97, and 193 because the ideal class number of $Q((-m)^{1/2})$ in these cases is 4.

References

1. P. Barrucand and H. Cohn, Note on primes of type $x^2 + 32y^2$, class number, and residuacity, *J. Reine Angew. Math.* **238** (1969), 67–70.
2. H. Cohn, "A Second Course in Number Theory," Wiley, New York, 1962.
3. D. Hilbert, Über den Dirichletschen biquadratischen Zahlkörper, *Math. Ann.* **45** (1894), 309–340; "Gesammelte Werke," Vol. I, pp. 24–52, Chelsea, New York, 1965).
4. D. Hilbert, Die Theorie der algebraischen Zahlkörper, *Jber. Deutsch. Math.-Verein.* **4** (1897), 175–546. "Gesammelte Werke," Vol. I, pp. 63–369, Chelsea, New York, 1965.
5. T. Nagell, "Introduction to Number Theory," second edition, Chelsea, New York, 1964.